ANTICIPATING WPS PIN VULNERABILITY TO SECURE WIRELESS NETWORK

Indra Dwi Rianto

Computer Science Department, School of Computer Science, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
indra.rianto@binus.edu

ABSTRACT

WiFi Protected Setup (WPS) is a standardized function supported by numerous vendors of wireless routers and access point to help set up connection to a wireless local area network. It is designed to simplify the set up and generally enabled by default. Due to design flaw, the WPS or QSS PIN is susceptible to a brute force attack. In this paper, we test the security vulnerability occurred, evaluate the performance and give recommendations to anticipate the attack.

Keywords: *wireless network, wifi protected setup, quick security setup*

ABSTRAK

WiFi Protected Setup (WPS) merupakan fitur standard yang disediakan oleh bermacam vendor wireless router dan access point untuk membantu set up koneksi kewireless local area network. WPS/QSS didesain untuk mempermudah set up dan umumnya aktif secara default. Dikarenakan ketidaksempurnaan design, PIN dari WPS atau QSS rapuh terhadap serangan brute force. Dalam paper ini, kami menguji kerentanan keamanan yang ditimbulkan, mengevaluasi kinerja dan memberikan rekomendasi untuk mengantisipasi serangan.

Kata kunci: *wireless network, wifi protected setup, quick security setup*

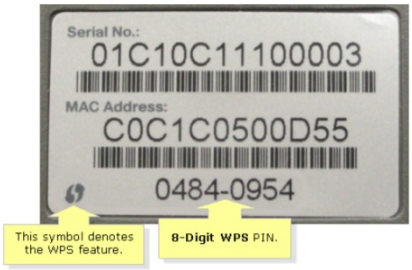
INTRODUCTION

Wireless network, also referred as Wi-Fi can be found almost everywhere. It is one of the easiest and least messy ways to network computers throughout your home, office, and many other public areas. Wi-Fi Protected Setup (WPS) is an optional certification program from the Wi-Fi Alliance designed to ease the task of setting up and configuring security on wireless local area networks. Introduced by the Wi-Fi Alliance in early 2007, it is an effort to get an industry-wide set of network setup solutions for homes and small office (SOHO) environment. WPS combines elements of Broadcom's Secure Easy Setup (SES), Buffalo's AOSS (AirStation One-Touch Secure System), Atheros' JumpStart, Intel's Smart Wireless Technology and Microsoft's WCN (Windows Connect Now) into a single method for getting a wireless network securely set up quickly and easily (Higgins, 2008).

There are two primary approaches to network setup within Wi-Fi Protected Setup: push-button and PIN entry. In push-button the user may connect multiple devices to the network and enable data encryption by pushing a button. The access point/wireless router will have a physical button, and other devices may have a physical or software-based button (Figure 1). Users should be aware that during the two-minute setup period which follows the push of the button, unintended devices could join the network if they are in range.

Figure 1 WPS push-button interface: physical and software-based button

For PIN entry, a unique 8-digit PIN (Personal Identification Number) will be required for each device to join the network. A fixed PIN label or sticker may be placed on a device, or a dynamic PIN can be generated and shown on a display (Figure 2). PIN is used to make sure the intended device is added to the network being set up and will help to avoid accidental or malicious attempts to add unintended devices to the network.



3. If your client asks for the Router's PIN number, enter this number **35128212** in your client device.

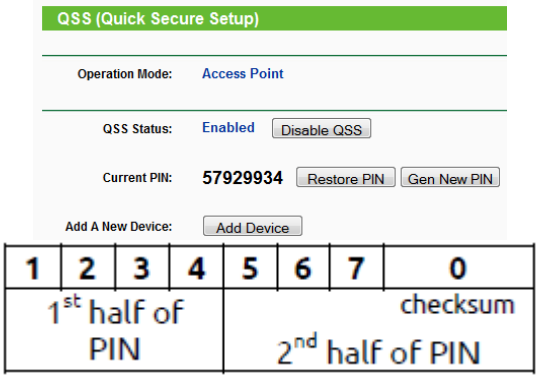


Figure 2 WPS PIN: static and dynamic

Basically, it is fairly simple to setup. Other devices or resources in local network or internet are connected to a wireless access point or router which broadcasts communication signal. Your device receives the signal and talk back to access point or router and you are connected. The problem with having the signal broadcast though is that it is difficult to contain where that signal may travel. How far the signal can travel depends on the access point's or router's performance. It may be accessible from other rooms, upstairs, downstairs, even unauthorized person.

However, it does not mean that we should not use wireless networking. We just have to be smart about it and take some basic precautions to make it more difficult for curious seekers to get into our personal information. This study contains information about one wireless network vulnerability called Wi-Fi Protected Setup (WPS), its attack evaluation and some recommendation to secure our wireless network from this vulnerability.

METHOD

The 8-digit numeric PIN is split into 2 sets of 4. The problem of the WPS authentication design is that if the first 4 digit have been found first, the router or access point proclaims whether the 4 digit is correct. This mark a checkpoint at which to save the progress before finding the last 4. So instead of having to guess an 8 digit combination, all that has to be guessed now is two 4 digit combinations and that takes considerably less time (Viehböck, 2011).

This form of authentication dramatically decreases the maximum possible authentication attempts needed from 10^8 (=100.000.000) to $10^4 + 10^4$ (=20.000). As the 8th digit of the PIN is always a checksum of digit one to digit seven, there are at most $10^4 + 10^3$ (=11.000) attempts needed to find the correct PIN.

In some cases, the authentication gets worse. Some routers do not even go into a lock-down state after consecutive failed attempts from a client; it allows as many guess as can be thrown at it. The lack of a proper lock out policy after a certain number of failed attempts to guess the PIN on some wireless routers makes this brute force attack that much more feasible.

The algorithm for doing the brute force attack is shown below (Figure 3).

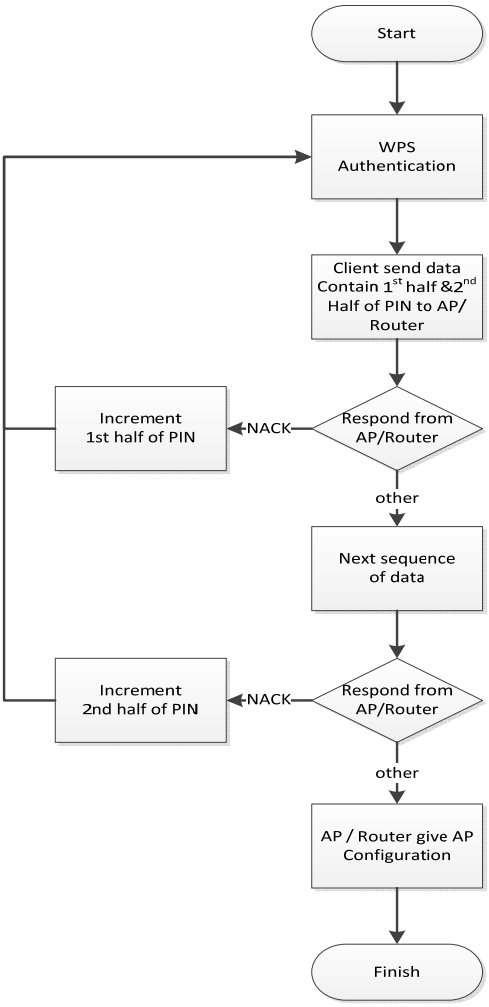


Figure 3 Flowchart on how brute force attack works on WPS PIN attack

To test the attack, we are using an open-source version of an attack tool, named Reaver (Heffner, 2011), that exploits the vulnerability. Reaver performs a brute force attack against the Router/AP, attempting every possible combination in order to guess the Router/AP's 8 digit pin number which can be discoveredwithin 11,000 attempts.

RESULTS AND DISCUSSION

We use Reaver1.4from Backtrack 5R3 (Pash, 2012) on the following devices (Tabel 1):

Tabel 1*Router and Access Point Tested*

Vendor	Series	FW-Version	WPS PIN
Linksys	WRT54GL	4.30.0	No, SES
Linksys	E2000	1.0.03	Yes
TP-Link	WA701N	3.9.12 Build 090929 Rel.39423n	Yes, QSS
Mikrotik	RB951-2n	RouterOS 5.16	No

The Linksys WRT54GL cannot be attacked using the WPS vulnerabilities since it using Broadcom's Secure Easy Setup (SES) which not use WPS PIN. SES use Push-Button method (Broadcom, 2012), therefore it can be attacked via WPS PIN.

Mikrotik RB951-2n also cannot be attacked using the WPS vulnerabilities since it does not implement WPS or WPS-like security method and Reaver will failed to associate connection with it.

The TP-Link WA701N use Quick Security Setup (QSS), which has the same function and complies with WPS. We managed to get the AP Pre-Shared Key (PSK) and PIN within four hours. One advantage of QSS is that you can re-generate your 8-digit PIN if you need it.

The Linksys E2000 use a Static PIN, which means it cannot be changed. We managed to get the AP Pre-Shared Key (PSK) and PIN within 9 hours (Figure 4).

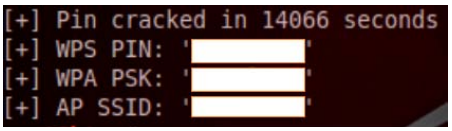


Figure 4 Reaver find the PIN and Wireless configuration given

In general, your distance to the Router/AP, signal strength, and its speed to process WPS request will determine how long the brute force attack need to take place. The other important factor is the actual WPS PIN. Since Reaver brute forcing incrementally on the first 4-digit and last 4-digit, the greater digit your actual PIN, the more time it will takes to successfully attempt with the right PIN. The WPS PIN in Linksys E2000 coincidently is more than two-times as the TP-Link WA701N's PIN (Figure 5).

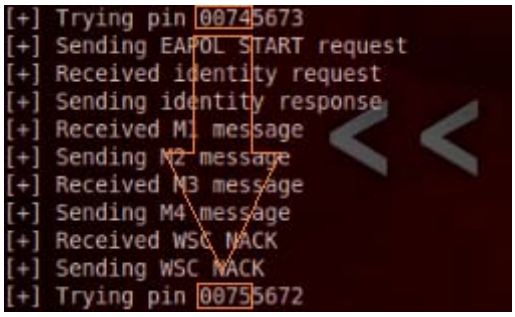


Figure 5 Reaver sequential increment on 1st half digit of WPS PIN

Having demonstrated the insecurity of WPS, we went into the Linksys E2000' administrative interface and try to turned the Wireless WPS off by select the Wireless Configuration to Manual (refer to figure 1) and reboot the device. With the Wireless Configuration set to Manual, then, we re-launched Reaver. However, apparently Linksys E2000' WPS interface still responded to Reaver's queries therefore still in danger of the attack. For, TP-Link WA701N's QSS, when it is disabled (refer to figure 2), Reaver failed to associate connection with it.

Reaver also managed to repeatedly cause the router or AP to be busy in responding WPS requestor essentially creating a denial of service attack.Both Linksys E2000and TP-Link WA701N web interface setup, take a longer time to load than normal. In Linksys E2000, account authentication processsometimes repeatedly become invalid even with the correct credentials.

CONCLUSION

The experimental result has shown that WPS PIN vulnerability can be exploited in less than one day. WPS can be disabled. However, some access points or router don't provide an option to disable WPS, or don't actually disable WPS when the owner tells it to. To correct this WPS issue all together will require a firmware update to the router or access point. If your router vendor has not released any firmware to address the vulnerabilities, you should use third party firmware like DD-WRT. Since it does not have support for WPS so they are not susceptible to the WPS attack. Please also be noted that your warranty will void if you re-flash your router with third party firmware.

REFERENCES

Broadcom. (2012-02-28). *SecureEasySetup Software*. Retrieved February 28, 2013 from Broadcom website: http://www.broadcom.com/products/secureeasysetup.php.

Heffner, Craig (2011). *Cracking WiFi Protected Setup with Reaver*. Retrieved February 28, 2013 from Tactical Network Solutions website: http://www.tacnetsol.com/news/2011/12/28/cracking-wifi-protected-setup-with-reaver.html.

Higgins, Tim. (2008). *How is WPS supposed to work?* Retrieved February 28, 2013 from SmallNetBuilder website: http://www.smallnetbuilder.com/wireless/wireless-features/30345-how-is-wps-supposed-to-work

Pash, Adams. (2012). *How to Crack a Wi-Fi Network's WPA Password with Reaver*. Retrieved February 28, 2013 from Lifehacker website: http://www.lifehacker.com.au/2012/01/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver/.

Viehböck, Stefan. (2011). *Brute forcing Wi-Fi Protected Setup.* Retrieved February 28, 2013 from http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

Wi-Fi Alliance. (2007). *Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi® Networks*. Retrieved February 28, 2013 from Wi-Fi Alliance website: http://www.wi-fi.org/files/wp_18_20070108_Wi-Fi_Protected_Setup_WP_FINAL.pdf.